IN THE UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN

ARTHUR WAGNER, individually and on behalf of all others similarly situated; Plaintiff, v. BENEFITS PARTNER, LLC, dba SALUS GROUP, Defendant.	Case No.: 2:25-cv-11219 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT AND JURY DEMAND

Plaintiff Arthur Wagner ("Plaintiff"), individually and on behalf of all others similarly situated, sues Defendant Benefits Partner, LLC, dba Salus Group ("Benefits Partner" or "Defendant"), to obtain damages, restitution, and injunctive relief for the Class, as defined below, from Defendant. Plaintiff makes the following allegations upon information and belief, except as to his own actions, the investigation of his counsel, and the facts that are a matter of public record.

I. INTRODUCTION

1. This class action arises out of the recent data security incident and data breach that was perpetrated against Defendant (the "Data Breach"), which held in its possession certain personally identifiable information ("PII") and protected health information ("PHI") (collectively, the "Private Information") of Plaintiff and other current and former customers of Defendant, the

putative class members ("Class"). Defendant's public notice of the Data Breach states that they determined their network had been accessed by an unknown actor on October 9, 2024.[1]

2. On April 7, 2025, Defendant mailed Plaintiff a letter advising him that the Private Information compromised in the Data Breach included certain personal or protected health information of his. This Private Information included but is not limited to his name, date of birth, Social Security number, and/or health insurance information. Notice of Data Breach, Exhibit A hereto.

3. The Private Information was acquired by cyber-criminals who perpetrated the attack and remains in the hands of those cyber-criminals.

4. The Data Breach resulted from Defendant's failure to implement adequate and reasonable cyber-security procedures and protocols necessary to protect individuals' Private Information with which they were entrusted for treatment.

5. Plaintiff brings this class action lawsuit on behalf of those similarly situated to address Defendant's inadequate safeguarding of Class Members' Private Information that they collected and maintained, and for failing to provide timely and adequate notice to Plaintiff and other Class Members that their information was subjected to unauthorized access by an unknown third party and precisely what specific type of information was accessed.

6. Defendant maintained the Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' Private Information was a known risk to

[1] Defendant Benefits Partner, Notice of Security Incident, *available at* https://thesalusgroup.com/security-incident/pdf (*last accessed* March 11, 2025).

Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

7. Defendant, through its employees, disregarded the rights of Plaintiff and Class Members (defined below) by, among other things, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its data systems were protected against unauthorized intrusions. Defendant also failed to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' Private Information and failed to take standard and reasonably available steps to prevent the Data Breach.

8. In addition, Defendant's employees failed to properly monitor the computer network and systems that housed the Private Information. Had Defendant's employees (presumably in the IT department) properly monitored its property, it would have discovered the intrusion sooner.

9. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct since the Private Information that Defendant collected and maintained is now in the hands of data thieves.

10. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes. These crimes include opening new financial accounts in Class Members' names, taking out loans in Class Members' names, using Class Members' information to obtain government benefits, filing false medical claims using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest.

11. Because of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and in the future closely monitor their financial accounts to guard against identity theft.

12. Plaintiff and Class Members may also incur out of pocket costs for, *e.g.*, purchasing credit monitoring services, credit freezes, credit reports, or other protective measures to deter and detect identity theft.

13. Through this Complaint, Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose Private Information was accessed during the Data Breach.

14. Plaintiff seeks remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, and injunctive relief including improvements to Defendant's data security systems, future annual audits, and adequate credit monitoring services funded by Defendant.

15. Accordingly, Plaintiff sues Defendant seeking redress for its unlawful conduct, and asserting claims for: (i) negligence, (ii) breach of implied contract, (iii) negligence *per se*, (iv) breach of fiduciary duty; and (v) unjust enrichment.

II. PARTIES

16. Plaintiff Arthur Wagner is and at all times mentioned herein was an individual citizen of Washington, residing in the city of Seattle.

17. Defendant Benefits Partner, LLC, dba Salus Group, is a domestic limited liability company headquartered at 38233 Mouns Road Building F, Sterling Heights, Michigan 48310.

18. Defendant's registered agent for service of process is C T Corporation System, 40600 Ann Arbor Road E, Suite 201, Plymouth, Michigan 48170.

III. JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are at least 100 putative Class Members and members of the proposed Class, including Plaintiff, are citizens of states different from Defendant. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).

20. This Court has jurisdiction over Defendant through its business operations in this District, the specific nature of which occurs in this District. Benefits Partner's principal place of business is in this District. Defendant intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(l) because a substantial part of the events giving rise to this action occurred in this District. Defendant is also based in this District, maintains Plaintiff's and Class Members' Private Information in this District, and has caused harm to Plaintiff and Class Members from and/or in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business

22. Defendant Benefits Partner is a boutique benefits and administration company based in Michigan. Founded in 2005, Benefits Partner was originally established as a Credit Union Service Organization that brought technology, employee benefits consulting, and administration to credit unions. [2]

23. Plaintiff and Class Members are current and former customers of Defendant.

24. As a condition of receiving benefits, Defendant required that its customers, including

[2] https://thesalusgroup.com/about/ (last viewed April 28, 2025).

Plaintiff and the Class Members, provide Defendant with their Private Information, including at least the following: names, dates of birth, Social Security numbers, health insurance information, and other sensitive information.

25. Defendant stored this Private Information in its information technology computer systems and servers, on information and belief located at its headquarters in Sterling Heights, Michigan.

26. On information and belief, the information held by Defendant in its computer systems at the time of the Data Breach included the unencrypted Private Information of Plaintiff and Class Members.

27. Upon information and belief, in the course of collecting Private Information from customers, including Plaintiff, Defendant promised to provide confidentiality and adequate security for the data it collected from them through its applicable privacy policy and through other disclosures in compliance with statutory privacy requirements and industry standards

28. Plaintiff and the Class Members, as customers of Defendant, relied on these promises and on this sophisticated business entity to keep their sensitive Private Information confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Customers, in general, demand security to safeguard their Private Information, especially when their Social Security numbers, PHI, and other sensitive Private Information is involved.

29. Plaintiff and the Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted it to Defendant absent a promise to safeguard that information.

30. Plaintiff and the Class Members provided their Private Information to Defendant with

the reasonable expectation and on the mutual understanding that Defendant would comply with its obligations to keep such Private Information confidential and secure from unauthorized access.

31. Defendant had a duty to adopt reasonable measures to protect the Private Information of Plaintiff and Class Members from involuntary disclosure to third parties. Defendant has a legal duty to keep consumer's Private Information safe and confidential.

32. Defendant had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep their Private Information confidential and to protect it from unauthorized access and disclosure.

33. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' Private Information, Defendant assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' Private Information from disclosure.

B. The Data Breach

34. Plaintiff and the proposed Class Members provided their Private Information to Defendant as a condition of receiving benefits. Defendant stored Plaintiff's and the Class Members' Private Information on its computer systems and servers.

35. Unfortunately, Defendant failed to take adequate measures to protect its current and former customers' Private Information stored on its computer servers, including failing to implement reasonable cybersecurity safeguards or policies to protect Private Information, and failing to supervise its information technology or data security agents and employees, or vendors, to prevent, detect, and stop breaches of its systems.

36. As a direct result of Defendant's failures, on October 9, 2024, cybercriminals infiltrated Defendant's systems, gained access to, and copied, the Private Information of Defendant's current

and former customers, Plaintiff and the Class Members, including but not limited to their names, Social Security Numbers, and PHI ("the Data Breach").[3]

37. A Data Breach occurs when cyber criminals intend to access and steal Private Information that has not been adequately secured by a business entity like Defendant.

38. Although the Data Breach occurred on October 9, 2024, Defendant would not notify impacted customers of the Data Breach until months later, on March 27, 2025.

39. According to Defendant, the Data Breach occurred as a result of its own staff having their email compromised.[4]

40. Only after almost six (6) months had passed did Defendant inform its affected customers, Plaintiff and the proposed Class Members, of the Data Breach in its letter dated April 7, 2025.

41. In the Data Breach Notice, Defendant stated that following the discovery of the Data Breach, it took steps to prevent future breaches, but these steps involve little more than increasing staff education and awareness, including "providing employees with further training on how to identify and avoid suspicious emails."[5]

42. Acknowledging the inadequate security of its systems prior to the Data Breach, Defendant stated in its Data Breach Notice that following discovery of the intrusion, it "implemented additional security controls in our email environment."[6]

---

[3] *See* Notice of Data Breach.

[4] *Id.*

[5] *Id.*

[6] *Id.*

43. Ultimately, Defendant encouraged Data Breach victims to "be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity."[7]

44. Finally, Defendant directed Data Breach victims to credit reporting agencies to help monitor their credit.[8]

45. Defendant has obfuscated the details of the Data Breach, omitting from its Data Breach Notice who perpetrated the Data Breach, why Defendant did not immediately detect the intrusion into its systems, why it took Defendant so long to notified impacted customers, and other key details.

46. On information and belief, based on the nature of the cyberattack, Plaintiff's and the members of the proposed Class Members' Private Information, unauthorizedly disclosed to third-party cybercriminals in the Data Breach, has now been, or will imminently be, posted to the Dark Web for public viewing and use, in the public domain, to be sold and utilized for fraudulent and criminal misuse.

47. As a result of the Data Breach, its victims face a lifetime risk of identity theft, as it includes sensitive information that cannot be changed, like their Social Security numbers. Defendant has offered nothing to compensate Plaintiff and the Class Members for their damages resulting from the Data Breach.

48. As a result of the Data Breach which Defendant permitted to occur by virtue of its inadequate data security practices, Plaintiff and the proposed Class Members have suffered injury and damages, as set forth herein.

---

[7] *Id.*

[8] *Id.*

49. The U.S. Department of Health and Human Services requires, "[i]f a breach of unsecured protected health information affects *500 or more individuals*, a covered entity must notify the Secretary of the breach without unreasonable delay and in *no case later than 60 calendar days* from the discovery of the breach."[9] Further, if "the number of individuals affected by a breach is uncertain at the time of submission, the covered entity should provide an estimate," and later provide an addendum or correction to HHS.[10]

50. Defendant's notice to HHS was dated April 8, 2025—almost six months after the Data Breach occurred. According to the online notice, the breach affected 40,177 individuals.[11]

51. Defendant had obligations created by HIPAA, contract, industry standards, common law, and representations made to Class Members, to keep Class Members' Private Information confidential and to protect it from unauthorized access and disclosure.

C. Data Breaches Are Preventable

52. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive information they were maintaining for Plaintiff and Class Members, causing the exposure of Private Information, such as encrypting the information or deleting it when it is no longer needed.

53. Defendant could have prevented this Data Breach by, among other things, properly encrypting or otherwise protecting their equipment and computer files containing Private Information.

---

[9] U.S. Department of Health and Human Services, *Submitting Notice of a Breach to the Secretary* (Feb. 27, 2023) https://www.hhs.gov/hipaa/for-professionals/breach-notification/breach-reporting/index.html (last viewed March 11, 2025) (emphasis added).

[10] *Id.*

[11] HHS Office for Civil Rights, Cases Currently Under Investigation, report dated April 8, 2025, *available at* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (*last accessed* April 28, 2025).

54. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[12]

55. To prevent and detect cyber-attacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders

[12] How to Protect Your Networks from RANSOMWARE, at 3, *available at:* https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view

supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[13]

56. To prevent and detect cyber-attacks or ransomware attacks, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

[13] *Id.* at 3-4.

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[14]

57. Given that Defendant was storing the Private Information of its current and former customers, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks.

58. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiff and Class Members.

59. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the Private Information of, upon information and belief, thousands to tens of thousands of individuals, including that of Plaintiff and Class Members.

[14] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/

D. Plaintiff's Experiences

60. Plaintiff Arthur Wagner is a customer of Defendant and provided his own Private Information to Defendant to obtain services for himself.

61. Thus, Defendant obtained and maintained Plaintiff's Private Information. As a result, Plaintiff was injured by Defendant's Data Breach.

62. Plaintiff provided his Private Information to Defendant and trusted the company would use reasonable measures to protect it according to Defendant's internal policies, as well as state and federal law. Defendant obtained and continues to maintain Plaintiff's Private Information and has a continuing legal duty and obligation to protect that Private Information from unauthorized access and disclosure.

63. Plaintiff reasonably understood that a portion of the funds paid to Defendant would be used to pay for adequate cybersecurity and protection of Private Information.

64. Plaintiff is very careful about sharing his sensitive PII and PHI. He has never knowingly transmitted unencrypted sensitive PII or PHI over the internet or any other unsecured source. Plaintiff also stores any documents containing his sensitive information in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

65. Plaintiff received a Notice of Data Breach in April of 2025.

66. Thus, on information and belief, Plaintiff's Private Information has already been published—or will be published imminently—by cybercriminals on the Dark Web.

67. Through its Data Breach, Defendant compromised Plaintiff's name and Social Security Number.

68. Plaintiff has already spent much time monitoring his account to protect himself and will continue to spend significant time and effort monitoring his accounts to protect himself from identity theft. After all, Defendant directed Plaintiff to take those steps in its Notice of Data Breach.

69. Plaintiff fears for his personal financial security and worries about what information was exposed in the Data Breach.

70. Because of Defendant's Data Breach, Plaintiff has suffered—and will continue to suffer from—anxiety, sleep disruption, stress, fear, and frustration. Such injuries go far beyond allegations of mere worry or inconvenience. Rather, Plaintiff's injuries are precisely the type of injuries that the law contemplates and addresses.

71. Plaintiff suffered actual injury from the exposure and theft of his Private Information—which violates his rights to privacy.

72. Plaintiff suffered actual injury in the form of damages to and diminution in the value of his Private Information. After all, Private Information is a form of intangible property—property that Defendant was required to adequately protect.

73. Plaintiff suffered imminent and impending injury arising from the substantially increased risk of fraud, misuse, and identity theft—all because Defendant's Data Breach placed Plaintiff's Private Information right in the hands of criminals.

74. Because of the Data Breach, Plaintiff anticipates spending considerable amounts of time and money to try and mitigate his injuries.

75. Today, Plaintiff has a continuing interest in ensuring that his Private Information—which, upon information and belief, remains backed up in Defendant's possession—is protected and safeguarded from additional breaches.

E. The Data Breach Was Foreseeable: Defendant Knew, or Should Have Known, of the Risk Because Insurance Entities in Possession of Private Information are Particularly Susceptible to Cyber Attacks

76. Defendant knew or should have known of the risk of a data breach, especially because insurance entities in possession of Private Information are particularly susceptible to cyber attacks.

77. Defendant's data security obligations were particularly important given the substantial increase in cyber-attacks and/or data breaches targeting insurance entities that collect and store Private Information, like Defendant, preceding the date of the breach.

78. Data breaches, including those perpetrated against insurance entities that store Private Information in their systems, have become widespread.

79. In 2023, an all-time high for data compromises occurred, with 3,205 compromises affecting 353,027,892 total victims. Of the 3,205 recorded data compromises, 809 of them, or 25.2% were in the medical or healthcare industry. The estimated number of organizations impacted by data compromises has increased by +2,600 percentage points since 2018, and the estimated number of victims has increased by +1400 percentage points. The 2023 compromises represent a 78-percentage point increase over the previous year and a 72-percentage point hike from the previous all-time high number of compromises (1,860) set in 2021.

80. In light of recent high profile cybersecurity incidents at other healthcare partner and provider companies, including HCA Healthcare (11 million patients, July 2023), Managed Care of North America (8 million patients, March 2023), PharMerica Corporation (5 million patients, March 2023), HealthEC LLC (4 million patients, July 2023), ESO Solutions, Inc. (2.7 million patients, September 2023), Prospect Medical Holdings, Inc. (1.3 million patients, July-August 2023), Defendant knew or should have known that its electronic records would be targeted by cybercriminals.

81. Indeed, cyber-attacks, such as the one experienced by Defendant, have become so notorious that the Federal Bureau of Investigation ("FBI") and U.S. Secret Service have issued a warning to potential targets so they are aware of, and prepared for, a potential attack. As one report explained, smaller entities that store Private Information are "attractive to ransomware criminals…because they often have lesser IT defenses and a high incentive to regain access to their data quickly."[15]

82. Additionally, as companies became more dependent on computer systems to run their business,[16] *e.g.*, working remotely as a result of the Covid-19 pandemic, and the Internet of Things ("IoT"), the danger posed by cybercriminals is magnified, thereby highlighting the need for adequate administrative, physical, and technical safeguards.[17]

83. Defendant knew and understood unprotected or exposed Private Information in the custody of insurance companies, like Defendant, is valuable and highly sought after by nefarious third parties seeking to illegally monetize that Private Information through unauthorized access.

84. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiff and Class Members and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

[15]https://www.law360.com/patientprotection/articles/1220974/fbi-secret-service-warn-of-targeted-ransomware?nl_pk=3ed44a08-fcc2-4b6c-89f0aa0155a8bb51&utm_source=newsletter&utm_medium=email&utm_campaign=patientprotection
[16]https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html
[17] https://www.picussecurity.com/key-threats-and-cyber-risks-facing-financial-services-and-banking-firms-in-2022

85. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

86. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the Private Information of Plaintiff and Class Members.

87. The ramifications of Defendant's failure to keep secure the Private Information of Plaintiff and Class Members are long lasting and severe. Once Private Information is stolen—particularly Social Security numbers and PHI—fraudulent use of that information and damage to victims may continue for years.

88. As an insurance entity in custody of the Private Information of its customers, Defendant knew, or should have known, the importance of safeguarding Private Information entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiff and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

F. Value of Private Information

89. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[18] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other

[18] 17 C.F.R. § 248.201 (2013).

things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[19]

90. The PII and PHI of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[20]

91. For example, Personal Information can be sold at a price ranging from $40 to $200.[21] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[22]

92. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. The popular person privacy and credit monitoring service LifeLock by Norton notes "Five Malicious Ways a Thief Can Use Your Social Security Number," including 1) Financial Identity Theft that includes "false applications for loans, credit cards or bank accounts in your name or withdraw money from your accounts, and which can encompass credit card fraud, bank fraud, computer fraud, wire fraud, mail fraud and employment fraud; 2) Government Identity Theft, including tax refund fraud; 3) Criminal Identity Theft, which involves using someone's stolen Social Security number as a "get out of jail free card;" 4) Medical Identity Theft, and 5) Utility Fraud.

---

[19] *Id.*
[20] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/
[21] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/
[22] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/

93. It is little wonder that courts have dubbed a stolen Social Security number as the "gold standard" for identity theft and fraud. Social Security numbers, which were compromised for some Class Members in the Data Breach, are among the worst kind of Private Information to have been stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change.

94. The greater efficiency of electronic health records brings the risk of privacy breaches. These electronic health records contain a lot of sensitive information (*e.g.,* patient data, patient diagnosis, lab results, medications, prescriptions, treatment plans, etc.) that is valuable to cybercriminals. One patient's complete record can be sold for hundreds of dollars on the dark web. As such, PHI/PII is a valuable commodity for which a "cyber black market" exists where criminals openly post stolen payment card numbers, Social Security numbers, and other personal information on several underground internet websites. Unsurprisingly, the healthcare industry is at high risk and is acutely affected by cyberattacks, like the Data Breach here.

95. Between 2005 and 2019, at least 249 million people were affected by healthcare data breaches.[23] Indeed, during 2019 alone, over 41 million healthcare records were exposed, stolen, or unlawfully disclosed in 505 data breaches.[24] In short, these sorts of data breaches are increasingly common, especially among healthcare systems, which account for 30.03 percent of overall health data breaches, according to cybersecurity firm Tenable.[25]

96. According to account monitoring company LogDog, coveted Social Security numbers were selling on the dark web for just $1 in 2016—the same as a Facebook account. That pales in

[23] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7349636/#B5-healthcare-08-00133/ (last accessed February 17, 2025).
[24] https://www.hipaajournal.com/december-2019-healthcare-data-breach-report/ (last accessed February 17, 2025).
[25] https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-incovid-19-era-breaches/ (last accessed February 17, 2025).

comparison with the asking price for medical data, which was selling for $300 and up.[26] Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[27]

97. Healthcare data is especially prized by data thieves. The National Association of Healthcare Access Management reports, "[p]ersonal medical data is said to be more than ten times as valuable as credit card information."[28]

98. "Medical identity theft is a growing and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam Dixon, executive director of World Privacy Forum. "Victims often experience financial repercussions and worse yet, they frequently discover erroneous information has been added to their personal medical files due to the thief's activities."[29]

99. A study by Experian found that the average cost of medical identity theft is "about $20,000" per incident and that most victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive to restore coverage.[30] Almost half of medical identity theft victims lose their healthcare coverage as a result of the incident, while nearly one-third of medical identity theft victims saw their insurance premiums rise, and 40 percent were never able to resolve their identity theft at all.[31]

---

[26] Paul Ducklin, *FBI "ransomware warning" for healthcare is a warning for everyone!*, Sophos (Oct. 29, 2020) *available at* https://news.sophos.com/en-us/2020/10/29/fbi-ransomware-warning-for-healthcare-is-a-warning-for-everyone/ (last visited December 11, 2024).

[27] Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), *available at* https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited December 11, 2024).

[28] Laurie Zabel, *The Value of Personal Medical Information: Protecting Against Data Breaches*, NAHAM Connections, *available at* https://www.naham.org/page/ConnectionsThe-Value-of-Personal-Medical-Information (last visited December 11, 2024).

[29] Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb. 7, 2014, https://khn.org/news/rise-of-indentity-theft/ (last accessed February 17, 2025).

[30] *See* Elinor Mills, "Study: Medical Identity Theft is Costly for Victims," CNET (Mar, 3, 2010), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last accessed February 17, 2025).

[31] *Id.; see also Healthcare Data Breach: What to Know About them and What to Do After One,* EXPERIAN, https://www.experian.com/blogs/ask-experian/healthcare-data-breach-what-to-know-about-them-and-what-to-do-after-one/ (last accessed February 17, 2025).

100. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change—Social Security numbers and names.

101. In recent years, the medical and financial services industries have experienced disproportionally higher numbers of data theft events than other industries. Defendant therefore knew or should have known this and strengthened its data systems accordingly. Defendant was put on notice of the substantial and foreseeable risk of harm from a data breach, yet it failed to properly prepare for that risk.

102. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their Private Information.

G. Defendant Failed to Comply with FTC Guidelines

103. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

104. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal patient information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks;

understand their network's vulnerabilities; and implement policies to correct any security problems.[32] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor incoming traffic for activity suggesting someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[33]

105. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

106. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect patient data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions also clarify the measures businesses must take to meet their data security obligations.

107. These FTC enforcement actions include actions against healthcare providers like Defendant. *See, e.g., In the Matter of LabMD, Inc., A Corp*, 2016-2 Trade Cas. (CCH) ¶ 79708, 2016 WL 4128215, at *32 (MSNET July 28, 2016) ("[T]he Commission concludes that LabMD's

[32] Federal Trade Commission, *Protecting Personal Information: A Guide for Business* (2016), *available at* www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited February 17, 2025).
[33] *Id*.

data security practices were unreasonable and constitute an unfair act or practice in violation of Section 5 of the FTC Act.").

108. As evidenced by the Data Breach, Defendant failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner.

109. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to patients' PII and PHI constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

110. Defendant was always fully aware of its obligation to protect the PII and PHI of its patients. Defendant was also aware of the significant repercussions that would result from its failure to do so.

111. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

H. Defendant Failed to Comply with HIPAA Guidelines

112. Defendant is a covered entity under HIPAA (45 C.F.R. § 160.102) and is required to comply with the HIPAA Privacy Rule and Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

113. Defendant is subject to the rules and regulations for safeguarding electronic forms of medical information pursuant to the Health Information Technology Act ("HITECH").[34] *See* 42 U.S.C. §17921, 45 C.F.R. § 160.103.

114. HIPAA's Privacy Rule or *Standards for Privacy of Individually Identifiable Health Information* establishes national standards for the protection of health information.

115. HIPAA's Privacy Rule or *Security Standards for the Protection of Electronic Protected Health Information* establishes a national set of security standards for protecting health information that is kept or transferred in electronic form.

116. HIPAA requires "compl[iance] with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

117. "Electronic protected health information" is "individually identifiable health information … that is (i) transmitted by electronic media; maintained in electronic media." 45 C.F.R. § 160.103.

118. HIPAA's Security Rule requires Defendant to do the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by its workforce.

[34] HIPAA and HITECH work in tandem to provide guidelines and rules for maintaining protected health information. HITECH references and incorporates HIPAA.

119. HIPAA also requires Defendant to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection of electronic protected health information." 45 C.F.R. § 164.306(e). Additionally, Defendant is required under HIPAA to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

120. HIPAA and HITECH also obligated Defendant to implement policies and procedures to prevent, detect, contain, and correct security violations, and to protect against uses or disclosures of electronic protected health information that are reasonably anticipated but not permitted by the privacy rules. *See* 45 C.F.R. § 164.306(a)(1) and § 164.306(a)(3); *see also* 42 U.S.C. §17902.

121. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, also requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and ***in no case later than 60 days following discovery of the breach***."[35]

122. HIPAA requires a covered entity to have and apply appropriate sanctions against patients of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of 45 C.F.R. Part 164, Subparts D or E. *See* 45 C.F.R. § 164.530(e).

123. HIPAA requires a covered entity to mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of 45 C.F.R. Part 164, Subpart E by the covered entity or its business associate. *See* 45 C.F.R. § 164.530(f).

[35] Breach Notification Rule, U.S. Dep't of Health & Human Services, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html (emphasis added).

124. HIPAA also requires the Office of Civil Rights ("OCR"), within the Department of Health and Human Services ("HHS"), to issue annual guidance documents on the provisions in the HIPAA Security Rule. *See* 45 C.F.R. §§ 164.302-164.318. For example, "HHS has developed guidance and tools to assist HIPAA covered entities in identifying and implementing the most cost effective and appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of e- and comply with the risk analysis requirements of the Security Rule." US Department of Health & Human Services, Security Rule Guidance Material.[36] The list of resources includes a link to guidelines set by the National Institute of Standards and Technology (NIST), which OCR says, "represent the industry standard for good business practices with respect to standards for securing e-." US Department of Health & Human Services, Guidance on Risk Analysis.[37]

I. Defendant Failed to Comply with Industry Standards

125. As shown above, experts studying cyber security routinely identify health insurance providers as being particularly vulnerable to cyberattacks because of the value of the PII and PHI which they collect and maintain.

126. Several best practices have been identified that a minimum should be implemented by health insurance providers like Defendant, including, but not limited to, educating all employees; using strong passwords; creating multi-layer security, including firewalls, antivirus, and anti-malware software; encryption, making data unreadable without a key; using multi-factor authentication; protecting backup data; and limiting which employees can access sensitive data.

[36] http://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html.
[37] https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

127. Other best cybersecurity practices that are standard in the insurance industry include installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

128. Moreover, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cybersecurity programs.

129. As evidenced by the Data Breach and its timeline, Defendant failed to follow some or all these industry best practices.

130. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

131. These foregoing frameworks are existing and applicable industry standards in the insurance industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

J. The Data Breach Caused Plaintiff and the Class Members Injury and Damages

132. Plaintiff and members of the proposed Class have suffered injury and damages from the unauthorized disclosure and misuse of their Private Information disclosed in the Data Breach that can be directly traced to Defendant, that has occurred, is ongoing, and/or will imminently occur.

133. Data Breaches such as the one experienced by Defendant's customers are especially problematic because of the disruption they cause to the daily lives of victims affected by the attack.

134. As stated prior, on information and belief, in the Data Breach, cybercriminals were able to access the Plaintiff's and the proposed Class Members' Private Information, which is now being used or will imminently be used for fraudulent purposes and/or has been sold for such purposes and posted on the Dark Web for sale, causing widespread injury and damages.

135. Once an individual's Private Information is for sale and access on the dark web, cybercriminals are able to use the stolen and compromised to gather and steal even more information.[38]

136. The ramifications of Defendant's failure to keep Plaintiff's and the Class's Private Information secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, or other information, such as addresses, without permission, to commit fraud or other crimes.

137. Because Defendant failed to prevent the Data Breach, Plaintiff and the proposed Class Members have suffered, will imminently suffer, and will continue to suffer injury-in-fact and damages, including but not limited to:

a. The loss of the opportunity to control how Private Information is used;

b. Unauthorized use of stolen Private Information;

c. Dramatic increase in spam telephone calls;

d. Emotional distress;

e. The compromise and continuing publication of their Private Information;

[38] Ryan Toohil, *What do Hackers do with Stolen Information*, Aura, (September 5, 2023) https://www.aura.com/learn/what-do-hackers-do-with-stolen-information (last visited February 18, 2025).

f. Out-of-pocket expenses associated with the prevention, detection, recovery, and remediation from identity theft or fraud, and for necessary credit monitoring and identity theft protection;

g. Lost opportunity costs and lost wages associated with the time and effort expended addressing and trying to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;

h. The diminution in value of their Private Information;

i. Delay in receipt of tax refund monies; and,

j. The continued risk to their PII and PHI, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the PII and PHI in its possession.

K. The Data Breach Caused Plaintiff and the Class Members Increased Risk of Identity Theft

138. Furthermore, the Data Breach has placed Plaintiff and the proposed Class Members at an increased risk of fraud and identity theft.

139. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendant's failures resulted in Plaintiff's and Class Members' PII and PHI falling into the hands of identity thieves.

140. The unencrypted PII and PHI of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

141. Further, the standard operating procedure for cybercriminals is to use some data, like the PII here, to access "Fullz packages" of that person to gain access to the full suite of additional

PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.

142. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

143. The development of "Fullz" packages means here that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

144. There are myriad dangers which affect victims of identity theft, including: cybercriminals opening new financial accounts, credit cards, and loans in victim's names; victim's losing health care benefits (medical identity theft); hackers taking over email and other accounts; time and effort to repair credit scores; losing home due to mortgage and deed fraud; theft of tax refunds; hackers posting embarrassing posts on victim's social media accounts; victims spending large amounts of time and money to recover their identities; experiencing psychological harm and emotional distress; victims becoming further victimized by repeat instances of identity theft and fraud; cybercriminals committing crimes in victim's names; victims' personal data circulating the Dark Web forever; victims receiving increased spam telephone calls and emails; victims' children or elderly parents having their identities stolen.

145. The FTC recommends that identity theft victims take several costly steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, seeking a credit freeze, and correcting their credit reports.[39]

146. Identity thieves use stolen PII such as Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

147. According to the Social Security Administration, each time an individual's Social Security number is compromised, "the potential for a thief to illegitimately gain access to bank accounts, credit cards, driving records, tax and employment histories and other private information increases." [40] Moreover, "[b]ecause many organizations still use SSNs as the primary identifier, exposure to identity theft and fraud remains."[41]

148. The Social Security Administration stresses that the loss of an individual's Social Security number, as experienced by Plaintiff and some Class Members, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause

[39] Federal Trade Commission, *What To Do Right Away* (2024), *available at* https://www.identitytheft.gov/Steps (last visited February 17, 2025).
[40] *See* https://www.ssa.gov/phila/ProtectingSSNs.htm#:~:text=An%20organization's%20collection%20and%20use,and%20other%20private%20information%20increases.
[41] *Id.*

a lot of problems.[42]

149. In fact, "[a] stolen Social Security number is one of the leading causes of identity theft and can threaten your financial health."[43] "Someone who has your SSN can use it to impersonate you, obtain credit and open bank accounts, apply for jobs, steal your tax refunds, get medical treatment, and steal your government benefits."[44]

150. Identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's PII to police during an arrest—resulting in an arrest warrant being issued in the victim's name. That can be even more problematic and difficult to remedy for someone who already has a criminal record.

151. Such fraud may go undetected until debt collection calls commence months, or even years, later. Stolen Social Security numbers also make it possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security Number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

152. It is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social

[42] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf
[43] *See* https://www.equifax.com/personal/education/identity-theft/articles/-/learn/social-security-number-identity-theft/
[44] *See* https://www.investopedia.com/terms/s/ssn.asp

Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

153. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[45]

154. The California state government warns patients that: "[o]riginally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information. With your name and SSN, an identity thief could open new credit and bank accounts, rent an apartment, or even get a job."[46]

155. Theft of PHI is also gravely serious: "A thief may use your name or health insurance numbers to see a doctor, get prescription drugs, file claims with your insurance provider, or get other care. If the thief's health information is mixed with yours, your treatment, insurance and payment records, and credit report may be affected."[47] Drug manufacturers, medical device manufacturers, pharmacies, hospitals and other healthcare service providers often purchase PII/PHI on the black market for the purpose of target marketing their products and services to the physical maladies of the data breach victims themselves. Insurance companies purchase and use wrongfully disclosed PHI to adjust their insureds' medical insurance premiums.

---

[45] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft

[46] *See* https://oag.ca.gov/idtheft/facts/your-ssn

[47] *See* Federal Trade Commission, *Medical Identity Theft*, *available at* http://www.consumer.ftc.gov/articles/0171-medical-identity-theft (last visited February 17, 2025).

156. Further, according to the Identity Theft Resource Center's 2021 Consumer Aftermath Report, identity theft victims suffer "staggering" emotional tolls: "For example, nearly 30% of victims have been the victim of a previous identity crime; an all-time high number of victims say they have contemplated suicide. Thirty-three percent reported not having enough money to pay for food and utilities, while 14% were evicted because they couldn't pay rent or their mortgage. Fifty-four percent reported feelings of being violated."

157. What's more, theft of PII and PHI is also gravely serious outside of the traditional risks of identity theft. In the last two decades, as more and more of our lives become interconnected through the lens of massively complex cloud computing, PII and PHI are valuable property rights.

158. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber black-market" for years.

159. Where the most PII and PHI belonging to Plaintiff and Class Members was accessible from Defendant's network, there is a strong probability that entire batches of stolen information have been dumped on the black market and are yet to be dumped on the black market, meaning Plaintiff and the Class Members are at an increased risk of fraud and identity theft for many years into the future.

160. Further, there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and between when Private Information and/or financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which studied data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

161. Thus, Plaintiff and the Class Members must vigilantly monitor their financial and credit accounts for many years to come.

162. Accordingly, the Data Breach has caused Plaintiff and the proposed Class Members a greatly increased risk of identity theft and fraud, in addition to the other injuries and damages set forth herein.

163. Defendant knew or should have known of these harms which would be caused by the Data Breach it permitted to occur and strengthened its data systems accordingly.

L. Loss of Time to Mitigate Risk of Identity Theft and Fraud

164. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that his or her Private Information was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and a Defendant arguing that the individual failed to mitigate damages.

165. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Social Security numbers or other government identification are affected.

166. By spending this time, data breach Plaintiff was not manufacturing his own harm, he was taking necessary steps at Defendant's direction and because the Data Breach included their Social Security numbers.

167. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the

Data Breach, such as contacting credit bureaus to place freezes on their accounts; changing passwords and re-securing their own computer networks; and checking their financial accounts for any indication of fraudulent activity, which may take years to detect.

168. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to his good name and credit record."[48]

M. Diminution in Value of Private Information

169. PII and PHI are valuable property rights.[49] Their value is axiomatic, considering the value of Big Data in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

170. An active and robust legitimate marketplace for Private Information exists. In 2019, the data brokering industry was worth roughly $200 billion.[50]

171. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[51]

---

[48] See U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

[49] *See, e.g.*, Randall T. Soma, et al, Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("Private Information") Equals the "Value" of Financial Assets, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("Private Information, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[50] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Oct. 18, 2024).

[51] https://datacoup.com/ (last visited Oct. 18, 2024).

172. Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive up to $50.00 a year.[52]

173. Conversely sensitive PII can sell for as much as $363 per record on the dark web according to the Infosec Institute.[53]

174. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

N. The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

175. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

176. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

177. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect

---

[52] Nielsen Computer & Mobile Panel, Frequently Asked Questions, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited April 28, 2025).

[53] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited April 28, 2025).

Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendant's failure to safeguard their Private Information.

V. DEFENDANT'S BREACH

178. Defendant breached its obligations to Plaintiff and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and its data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect patients' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that vendors with access to Defendant's protected health data employed reasonable security procedures;

e. Failing to ensure the confidentiality and integrity of electronic PHI they created, received, maintained, and/or transmitted, in violation of 45 C.F.R. § 164.306(a)(1);

f. Failing to implement technical policies and procedures for electronic information systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights in violation of 45 C.F.R. § 164.312(a)(1);

g. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 C.F.R. § 164.308(a)(1)(i);

h. Failing to implement procedures to review records of information system activity regularly, such as audit logs, access reports, and security incident tracking reports in violation of 45 C.F.R. § 164.308(a)(1)(ii)(D);

i. Failing to protect against reasonably anticipated threats or hazards to the security or integrity of electronic PHI in violation of 45 C.F.R. § 164.306(a)(2);

j. Failing to protect against reasonably anticipated uses or disclosures of electronic PHI that are not permitted under the privacy rules related to individually identifiable health information in violation of 45 C.F.R. § 164.306(a)(3);

k. Failing to ensure compliance with HIPAA security standard rules by Defendant's workforce in violation of 45 C.F.R. § 164.306(a)(4);

l. Failing to train all members of Defendant's workforce effectively on the policies and procedures about PHI as necessary and appropriate for the members of its workforces to carry out their functions and to maintain security of PHI, in violation of 45 C.F.R. § 164.530(b); and/or

m. Failing to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as they had not encrypted the electronic PHI as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key" (45 C.F.R. § 164.304, definition of "encryption").

179. As the result of computer systems needing security upgrading, inadequate vetting of vendors, inadequate procedures for handling emails containing malignant computer code, and inadequately trained employees who opened files containing malignant computer code, Defendant negligently and unlawfully failed to safeguard Plaintiff's and Class Members' Private Information.

180. Plaintiff and Class Members now face an increased risk of fraud and identity theft.

VI. PLAINTIFF'S AND CLASS MEMBERS' DAMAGES

181. To date, Defendant has done little to provide Plaintiff and Class Members with relief for the damages they have suffered because of the Data Breach, including, but not limited to, the costs and loss of time they incurred because of the Data Breach. Defendant has only offered 24 months of inadequate credit monitoring services, despite Plaintiff and Class Members being at risk of identity theft and fraud for the remainder of their lifetimes.

182. The 24 months of credit monitoring offered to persons whose Private Information was compromised is wholly inadequate as it fails to provide for the fact that victims of data breaches and other unauthorized disclosures commonly face multiple years of ongoing identity theft and financial fraud.

183. Defendant's credit monitoring advice to Plaintiff and Class Members places the burden on Plaintiff and Class Members, rather than on Defendant, to investigate and protect themselves from Defendant's tortious acts resulting in the Data Breach.

184. Plaintiff and Class Members have been damaged by the compromise and exfiltration of their Private Information in the Data Breach, and by the severe disruption to their lives as a direct and foreseeable consequence of this Data Breach.

185. Plaintiff's Private Information was compromised and exfiltrated by cyber-criminals as a direct and proximate result of the Data Breach.

186. Plaintiff was damaged in that his Private Information is in the hands of cyber criminals.

187. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been placed at an actual, present, immediate, and continuing increased risk of harm from fraud and identity theft.

188. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have been forced to expend time dealing with the effects of the Data Breach.

189. Plaintiff and Class Members face substantial risk of out-of-pocket fraud losses such as loans opened in their names, medical services billed in their names, and similar identity theft.

190. Plaintiff and Class Members face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiff and Class Members.

191. Plaintiff and Class Members may also incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

192. Plaintiff and Class Members also suffered a loss of value of their Private Information when it was acquired by cyber thieves in the Data Breach. Many courts have recognized the propriety of loss of value damages in related cases.

193. Plaintiff and Class Members have spent and will continue to spend significant amounts of time to monitor their financial accounts and records for misuse.

194. Plaintiff and Class Members have suffered or will suffer actual injury as a direct result of the Data Breach. Many victims suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach relating to:

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Purchasing credit monitoring and identity theft prevention;

d. Addressing their inability to withdraw funds linked to compromised accounts;

e. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

f. Placing "freezes" and "alerts" with credit reporting agencies;

g. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

h. Contacting financial institutions and closing or modifying financial accounts;

i. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

j. Paying late fees and declined payment fees imposed because of failed automatic payments that were tied to compromised cards that had to be cancelled; and

k. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

195. Moreover, Plaintiff and Class Members have an interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further

breaches by implementing security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing personal and financial information is inaccessible online and that access to such data is password protected.

196. Further, because of Defendant's conduct, Plaintiff and Class Members are forced to live with the anxiety that their Private Information —which contains the most intimate details about a person's life—may be disclosed to the entire world, thereby subjecting them to embarrassment and depriving them of any right to privacy whatsoever.

197. As a direct and proximate result of Defendant's actions and inactions, Plaintiff and Class Members have suffered anxiety, emotional distress, and loss of privacy, and are at an increased risk of future harm.

VII. CLASS ACTION ALLEGATIONS

198. This action is brought and may be properly maintained as a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure.

199. Plaintiff brings this action on behalf of himself and on behalf of all other persons similarly situated.

200. Plaintiff proposes the following Class definition, subject to amendment as appropriate:

> **All persons whose Private Information was compromised because of the October 9, 2024, Data Breach (the "Class").**

201. Excluded from the Class are Defendant's officers and directors, and any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are Members of the judiciary to whom this case is assigned, their families and Members of their staff.

202. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. The exact number of Class Members is unknown to Plaintiff now, but Defendant has provided notice to HHS that 40,177 individuals were affected.

203. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiff's and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach adhered to industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Plaintiff and Class Members suffered legally cognizable damages from Defendant's misconduct;

i. Whether Defendant's conduct was negligent;

j. Whether Defendant's conduct was *per se* negligent;

k. Whether Defendant was unjustly enriched;

l. Whether Defendant failed to provide notice of the Data Breach promptly; and

m. Whether Plaintiff and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

204. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's Private Information, like that of every other Class member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, among other things, all Class Members were injured through the common misconduct of Defendant. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and no defenses are unique to Plaintiff. Plaintiff's claims and those of Class Members arise from the same operative facts and are based on the same legal theories.

205. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiff's Counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

206. Predominance. Defendant has engaged in a common course of conduct toward Plaintiff and Class Members, in that all Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

207. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for

Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

208. Defendant has acted on grounds that apply generally to the Class as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

209. Likewise, issues that will arise in this case are appropriate for class certification because such issues are common to the Class, the resolution of which would advance matter and the parties' interests therein. Such issues include, but are not limited to:

a. Whether Defendant failed to timely notify the public of the Data Breach;

b. Whether Defendant owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Private Information;

c. Whether Defendant's security measures to protect its data systems were reasonable considering best practices recommended by data security experts;

d. Whether Defendant's failure to institute adequate protective security measures amounted to negligence;

e. Whether Defendant failed to take commercially reasonable steps to safeguard consumer Private Information; and

f. Whether adherence to FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

210. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses affected by the Data Breach. Class Members have already been preliminarily identified and sent notice of the Data Breach by Defendant.

VIII. CAUSES OF ACTION

FIRST COUNT
NEGLIGENCE
(On Behalf of Plaintiff and All Class Members)

211. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

212. Defendant required Plaintiff and Class Members to submit non-public personal information to obtain benefits.

213. By collecting and storing this data in Defendant's computer property, and sharing it and using it for commercial gain, Defendant had a duty of care to use reasonable means to secure and safeguard its computer property—and Class Members' Private Information held within it—to prevent disclosure of the information, and to safeguard the information from theft. Defendant's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period and to give prompt notice to those affected in the case of a Data Breach.

214. Defendant owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected the Private Information.

215. Defendant's duty of care to use reasonable security measures arose because of the special relationship that existed between Defendant and its customers, which is recognized by laws and regulations including, but not limited to, HIPAA, as well as common law. Defendant could ensure that its systems were sufficient to protect against the foreseeable risk of harm to Class Members from a data breach.

216. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or

disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all the healthcare information at issue constitutes "protected health information" within the meaning of HIPAA.

217. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

218. Defendant's duty to use reasonable care in protecting confidential data arose not only because of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

219. Defendant breached its duties, and thus was negligent, by failing to use reasonable measures to protect Class Members' Private Information. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class Members' Private Information;

b. Failing to adequately monitor the security of its networks and systems;

c. Failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

d. Allowing unauthorized access to Class Members' Private Information;

e. Failing to detect timely that Class Members' Private Information had been compromised;

f. Failing to timely notify Class Members about the Data Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages; and

g. Failing to secure its stand-alone personal computers, such as the reception desk computers, even after discovery of the data breach.

220. It was foreseeable that Defendant's failure to use reasonable measures to protect Class Members' Private Information would result in injury to Class Members. Further, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the insurance industry.

221. It was therefore foreseeable that the failure to adequately safeguard Class Members' Private Information would result in one or more types of injuries to Class Members.

222. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered because of the Data Breach.

223. Defendant's negligent conduct is ongoing, in that they still hold the Private Information of Plaintiff and Class Members in an unsafe and unsecure manner.

224. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) provide adequate credit monitoring to all Class Members.

SECOND COUNT
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and All Class Members)

225. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

226. When Plaintiff and Class Members provided their Private Information to Defendant in exchange for insurance and benefits with Defendant, they entered implied contracts with Defendant under which Defendant agreed to reasonably protect such information.

227. Defendant solicited, offered, and invited Class Members to provide their Private Information as part of Defendant's regular business practices. Plaintiff and Class Members accepted Defendant's offers and provided their Private Information to Defendant.

228. In entering such implied contracts, Plaintiff and Class Members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, including HIPAA, and adhered to industry standards.

229. Plaintiff and Class Members paid money to Defendant with the reasonable belief and expectation that Defendant would use part of its earnings to obtain adequate data security. Defendant failed to do so.

230. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

231. Plaintiff and Class Members would not have entrusted their Private Information to Defendant in the absence of its implied promise to monitor its computer systems and networks to ensure that they adopted reasonable data security measures.

232. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

233. Defendant breached its implied contracts with Class Members by failing to safeguard and protect their Private Information.

234. As a direct and proximate result of Defendant's breach of the implied contracts, Class Members sustained damages as alleged here, including the loss of the benefit of the bargain.

235. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered because of the Data Breach.

236. Plaintiff and Class Members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen its data security systems and monitoring procedures; (ii) submit to future

annual audits of those systems and monitoring procedures; and (iii) immediately provide adequate credit monitoring to all Class Members.

THIRD COUNT
NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and All Class Members)

237. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

238. Under the Federal Trade Commission Act, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

239. Under HIPAA, 42 U.S.C. § 1302d, et seq., Defendant had a duty to implement reasonable safeguards to protect Plaintiff's and Class Members' Private Information.

240. Under HIPAA, Defendant had a duty to render the electronic PHI they maintained unusable, unreadable, or indecipherable to unauthorized individuals, as specified in the HIPAA Security Rule by "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key." See definition of encryption at 45 C.F.R. § 164.304.

241. Defendant breached its duties to Plaintiff and Class Members under the Federal Trade Commission Act and HIPAA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiff's and Class Members' Private Information.

242. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

243. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

244. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendant's breach of its duties. Defendant knew or should have known that

by failing to meet its duties, and that Defendant's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their Private Information.

245. As a direct and proximate result of Defendant's negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

FOURTH COUNT
BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and All Class Members)

246. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

247. Defendant became guardian of Plaintiff's and Class Members' Private Information, creating a special relationship between Defendant and Plaintiff and Class Members.

248. As such, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiff and Class Members, (1) for the safeguarding of Plaintiff's and Class Members' Private Information; (2) to timely notify Plaintiff and Class Members of a Data Breach and disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

249. Defendant has a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of Defendant's relationship with its patients, in particular, to keep secure their Private Information.

250. Defendant breached its fiduciary duties to Plaintiff and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiff's and Class Members' Private Information.

251. Defendant breached its fiduciary duties owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach.

252. Defendant breached its fiduciary duties to Plaintiff and Class Members by otherwise failing to safeguard Plaintiff's and Class Members' Private Information.

253. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the compromise, publication, and/or theft of their Private Information;

c. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information;

d. lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

e. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession;

f. future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the rest of the lives of Plaintiff and Class Members; and

g. the diminished value of Defendant's services they received.

254. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

FIFTH COUNT
UNJUST ENRICHMENT
(On Behalf of Plaintiff and All Class Members)

255. Plaintiff re-alleges and incorporates the above allegations as if fully set forth herein.

256. Plaintiff brings this claim individually and on behalf of all Class Members. This count is pled in the alternative to the breach of contract count above.

257. Upon information and belief, Defendant funds its data security measures entirely from its general revenue, including payments made by or on behalf of Plaintiff and the Class Members.

258. As such, a portion of the payments made by or on behalf of Plaintiff and the Class Members is to be used to provide a reasonable level of data security, and the portion of each payment made that is allocated to data security is known to Defendant.

259. Plaintiff and Class Members conferred a monetary benefit on Defendant. They bought services from Defendant and provided labor to Defendant and/or its agents and in so doing provided Defendant with their Private Information. In exchange, Plaintiff and Class Members should have received from Defendant the services that were the subject of the transaction and had their Private Information protected with adequate data security.

260. Defendant knew that Plaintiff and Class Members conferred a benefit which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiff and Class Members for business purposes.

261. Defendant enriched itself by saving the costs Defendant reasonably should have expended on data security measures to secure Plaintiff's and Class Members' Personal Information. Rather than providing a reasonable level of security that would have prevented the hacking incident, Defendant instead calculated to increase its own profits at the expense of Plaintiff and Class Members by using cheaper, ineffective security measures. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decision to prioritize its own profits over the requisite security.

262. Under the principles of equity and good conscience, Defendant should not be permitted to retain the money belonging to Plaintiff and Class Members, because Defendant failed

to implement appropriate data management and security measures that are mandated by industry standards.

263. Defendant failed to secure Plaintiff's and Class Members' Private Information and thus did not provide full compensation for the benefit Plaintiff and Class Members provided.

264. Defendant acquired the Private Information through inequitable means in that they failed to disclose the inadequate security practices alleged.

265. If Plaintiff and Class Members knew that Defendant had not reasonably secured their Private Information, they would not have agreed to provide their Private Information to Defendant.

266. Plaintiff and Class Members have no adequate remedy at law.

267. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will suffer injury, including but not limited to:

a. actual identity theft;

b. the loss of the opportunity of how their Private Information is used;

c. the compromise, publication, and/or theft of their Private Information;

d. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their Private Information;

e. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft;

f. the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information in its continued possession; and

g. future costs in terms of time, effort, and money to be expended to prevent, detect, contest, and repair the effect of the Private Information compromised because of the Data Breach for the rest of the lives of Plaintiff and Class Members.

268. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

269. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they unjustly received from them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiff and Class Members overpaid for Defendant's services.

IX. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and the Class described above seeks the following relief:

a. For an Order certifying this action as a class action, defining the Class as requested herein, appointing Plaintiff and his counsel to represent the Class, and finding that Plaintiff is a proper representative of the Class requested herein;

b. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein relating to the misuse and/or disclosure of Plaintiff's and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and Class Members;

c. For equitable relief compelling Defendant to use appropriate methods and policies related to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained because of Defendant's wrongful conduct;

e. For an order directing Defendant to pay for not less than ten years of credit monitoring services for Plaintiff and the Class;

f. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g. For an award of punitive damages, as allowable by law;

h. For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i. Pre- and post-judgment interest on any amounts awarded; and

j. Any other relief that this court may deem just and proper.

X. JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

DATED: April 28, 2025

Respectfully submitted,

/s/ Sean Short
Sean Short
Arkansas Bar No. 2015079
sean@sanfordlawfirm.com
SANFORD LAW FIRM, PLLC
Kirkpatrick Plaza
10800 Financial Centre Pkwy, Suite 510
Little Rock, Arkansas 72211
Telephone: (800) 615-4946
Facsimile: (888) 787-2040

Leigh S. Montgomery*
Texas Bar No. 24052214
lmontgomery@eksm.com
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Phone: (888) 350-3931
Fax: (888) 276-3455

ATTORNEYS FOR PLAINTIFF AND THE PUTATIVE CLASS

(* denotes *pro hac vice* forthcoming)